U.S. Environmental Protection Agency
Office of Inspector General

15-P-0073
February 3, 2015

At a Glance

Why We Did This Review

We performed this audit to assess the U.S. Chemical Safety and Hazard Investigation Board's (CSB's) compliance with the Federal Information Security Management Act of 2002 (FISMA).

FISMA requires federal agencies to develop an information security program that protects the operations and assets of the agency. The Inspector General is to perform an annual independent evaluation of the security program.

This report addresses the following CSB goal:

- *Preserve the public trust by maintaining and improving organizational excellence.*

Send all inquiries to our public affairs office at (202) 566 2391 or visit www.epa.gov/oig.

The full report is at:
www.epa.gov/oig/reports/2015/20150203-15-P-0073.pdf

Key Aspects of CSB Information Security Program Need Improvement

What We Found

CSB should improve key aspects of its information security program to better manage practices related to information security planning, physical and environmental security controls, its vulnerability testing process, and internal controls over its information technology inventory.

CSB's ability to increase its situational awareness and reduce risk exposure is challenged by its lack of a real-time continuous monitoring strategy.

The National Institute of Standards and Technology provides guidance for how federal organizations should continuously monitor security control effectiveness and remediate vulnerabilities. Office of Management and Budget Circular A-123, *Management's Responsibility for Internal Control*, provides guidance on how federal programs should develop internal controls to ensure that they achieve their desired objectives.

Federal information systems are subject to threats, including environmental disruptions, human and/or machine errors, and purposeful attacks. If CSB information technology inventory is stolen or its network breached, CSB data, information and configurations may be exposed.

Recommendations and Planned CSB Corrective Actions

We recommend that CSB update and maintain its system security plan, implement a risk management framework, create a visitor access record for the server room, formally accept risk of unimplemented privacy and security controls and vulnerabilities, and develop a process for orderly shutdown of critical information technology assets. We also recommend that CSB create plans to remediate systems with known vulnerabilities and expand its monthly vulnerability testing process to include all assets attached to the network. Further, we recommend that CSB improve its inventory control practices to ensure personnel do not perform incompatible duties, provide policies and procedures for safeguarding inventory, review and document lost items, and recover costs for lost items due to employee negligence.

CSB concurred with our recommendations and provided corrective actions with estimated completion dates for each recommendation. All 17 recommendations we made are resolved and corrective actions are completed or ongoing.

Noteworthy Achievements

CSB took significant action to implement processes to eliminate excessive electronic device inventory and to document management's justification for assigning multiple electronic devices to certain CSB personnel.